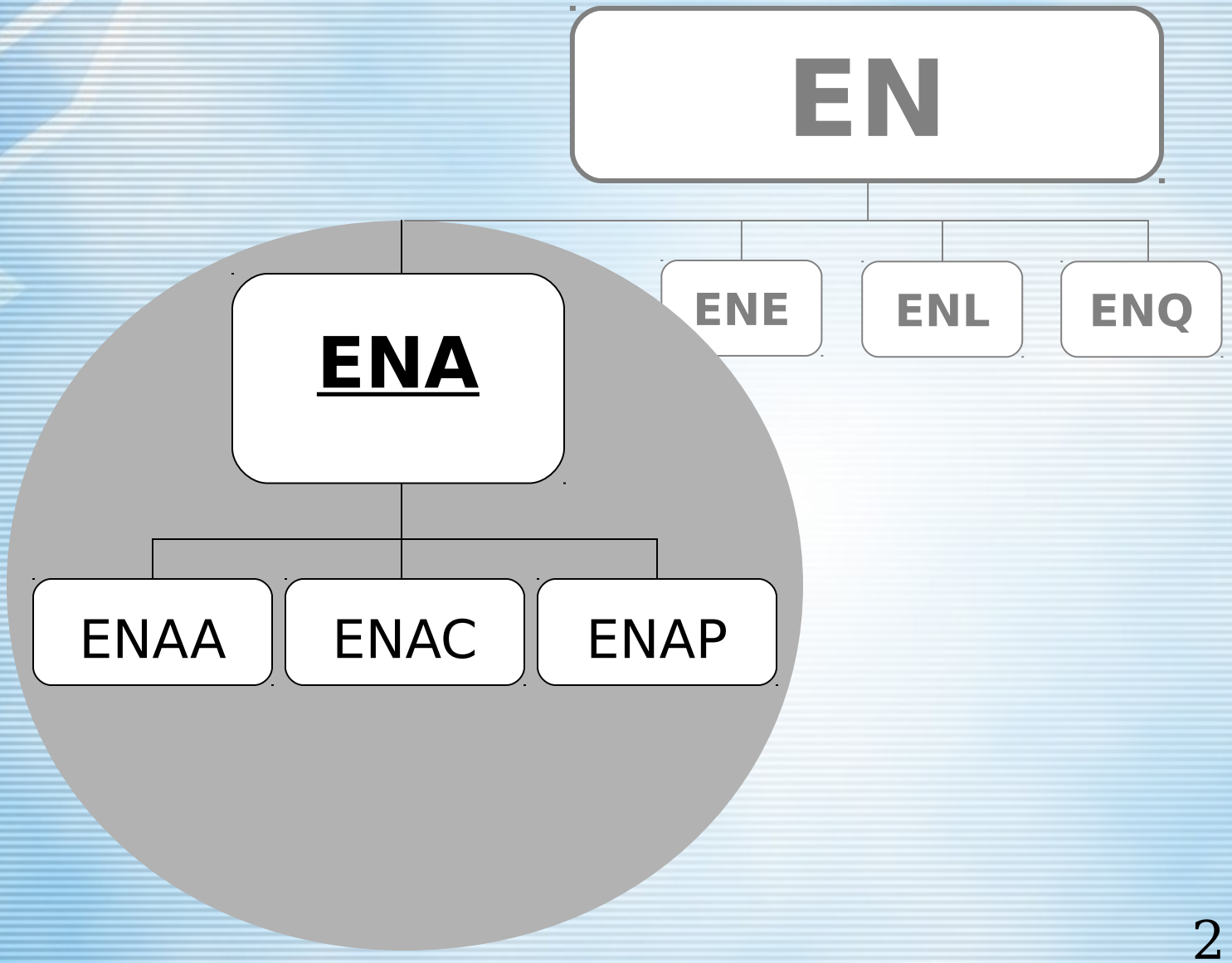
ENA
Engineering
Security Division

Presented by: John Margetson, SSG/

The Information Technology Center of Excellence for the Warfighter

ENA Org Chart



ENAA Capabilities

ENAA – System Security Authorization Agreement (SSAA)

- SSAA Development – To include developing full DoD Information Technology Security Certification and Accreditation Process (DITSCAP) SSAAs, updates to current SSAAs, and provide Security Testing and Evaluation (ST&E) services.

- SSAA Compliance Review - Thorough examination of SSAA documentation to ensure compliance with DoD, AF, Public Law, etc. requirements and validation that adequate security safeguards have been incorporated in the application design. ENAA compliance review validates accreditation recommendations to the DAA.

ENAC Capabilities

ENAC – SSG Security Policy and Compliance and SSAA Compliance

- System Security Authorization Agreement (SSAA) Review – Review to ensure compliance with Public Law, DoD, and AF requirements to ensure adequate security safeguards have been incorporated into IT systems.

- Security Policy Compliance Assessment (SPCA) - (Accomplished in conjunction with SSAA Compliance Reviews) ENAC holds an AFCA SPCA license and serves as the AFCA agent for CoN recommendations.

- Software Engineering Process (SEP) Audit - ENAC supports the SEP process by conducting the security portion of the scheduled SEP audits.

- Security Policy - Policy interpretation, guidance and issue resolution, and security consultation support.

ENAP Capabilities

ENAP – Command, Control, Communications, Computers, and Intelligence Support Plan (C4ISP) Development Activities

- C4ISP Development - The support plan will be developed to document the current or to-be system. Current DoD and AF guidance will be used as reference for format and content. Any and all existing system documentation will be used in-conjunction with consultation with the developers and functionals.

- C4ISP/CoN/CtO issues - ENAP will continue to work with the involved agencies (both internal and external) to interpret policy and guidance and provide input to the related processes at all levels. This support ranges from participating in meetings, conferences and PMRs as requested by the PMO, as well as policy clarification. The ENAP staff will also work on behalf of the customer to resolve any C4ISP/CoN/CtO issues locally or with activities outside the SSG community.

COTS Security

Some References

- All IA and IA-enable IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11.
  - International Common Criteria
  - NIST/NSA National Information Assurance Partnership (NIAP)
  - NIST Federal Information Processing Standards (FIPS)

- All IA and IA-enabled IT products incorporated into DoD information systems shall be configured IAW DoD guidelines (DODD 8500.1).
  - http://iase.disa.mil
  - http://www.nsa.gov

- AFI 33-202, Network and Computer Security
- AFI 33-223, Identification and Authentication
- AFM 33-229, Controlled Access Protection

Questions ?